

**FIPS 140-2 Non-Proprietary Security Policy
for Aruba AP-304, AP-305, AP-314, AP-315, AP-334, AP-
335, AP-365, and AP-367 Wireless Access Points**


**Version 1.4
February 2020**



**3333 Scott Blvd.
Santa Clara, CA 95054**

Copyright

© 2020 Aruba an HP Enterprise Company. Aruba trademarks include

 , Aruba Networks®, Aruba Wireless Networks®, the registered Aruba the Mobile Edge Company logo, Aruba Mobility Management System®, Mobile Edge Architecture®, People Move. Networks Must Follow®, RFProtect®, Green Island®. All rights reserved. All other trademarks are the property of their respective owners. Open Source Code

Certain Aruba products include Open Source software code developed by third parties, including software code subject to the GNU General Public License (GPL), GNU Lesser General Public License (LGPL), or other Open Source Licenses. The Open Source code used can be found at this site:

http://www.arubanetworks.com/open_source

Legal Notice

The use of Aruba switching platforms and software, by all individuals or corporations, to terminate other vendors' VPN client devices constitutes complete acceptance of liability by that individual or corporation for this action and indemnifies, in full, Aruba Networks, Inc. from any and all legal actions that might be taken against it with respect to infringement of copyright on behalf of those vendors.

Warranty

This hardware product is protected by the standard Aruba warranty of one year parts/labor. For more information, refer to the ARUBACARE SERVICE AND SUPPORT TERMS AND CONDITIONS.

Altering this device (such as painting it) voids the warranty.

1	INTRODUCTION	5
1.1	ACRONYMS AND ABBREVIATIONS	5
2	PRODUCT OVERVIEW	6
2.1	AP-304.....	6
2.1.1	<i>Physical Description</i>	7
2.1.1.1	Dimensions/Weight	7
2.1.1.2	Interfaces	7
2.2	AP-305.....	8
2.2.1	<i>Physical Description</i>	8
2.2.1.1	Dimensions/Weight	9
2.2.1.2	Interfaces	9
2.3	AP-314.....	10
2.3.1	<i>Physical Description</i>	10
2.3.1.1	Dimensions/Weight	11
2.3.1.2	Interfaces	11
2.4	AP-315.....	12
2.4.1	<i>Physical Description</i>	12
2.4.1.1	Dimensions/Weight	13
2.4.1.2	Interfaces	13
2.5	AP-334.....	14
2.5.1	<i>Physical Description</i>	14
2.5.1.1	Dimensions/Weight	15
2.5.1.2	Interfaces	16
2.6	AP-335.....	17
2.6.1	<i>Physical Description</i>	17
2.6.1.1	Dimensions/Weight	18
2.6.1.2	Interfaces	18
2.7	AP-365.....	19
2.7.1	<i>Physical Description</i>	19
2.7.1.1	Dimensions/Weight	20
2.7.1.2	Interfaces	20
2.8	AP-367.....	21
2.8.1	<i>Physical Description</i>	21
2.8.1.1	Dimensions/Weight	22
2.8.1.2	Interfaces	22
3	MODULE OBJECTIVES	23
3.1	SECURITY LEVELS	23

3.2	PHYSICAL SECURITY	23
3.2.1	<i>Applying TELs</i>	23
3.2.2	<i>TELs Placement</i>	24
3.2.2.1	TELs Placement on the AP-304.....	24
3.2.2.2	TELs Placement on the AP-305.....	25
3.2.2.3	TELs Placement on the AP-314.....	26
3.2.2.4	TELs Placement on the AP-315.....	27
3.2.2.5	TELs Placement on the AP-334.....	28
3.2.2.6	TELs Placement on the AP-335.....	29
3.2.2.7	TELs Placement on the AP-365.....	30
3.2.2.8	TELs Placement on the AP-367.....	31
3.2.3	<i>Inspection/Testing of Physical Security Mechanisms</i>	32
3.3	OPERATIONAL ENVIRONMENT.....	32
3.4	LOGICAL INTERFACES	32
4	ROLES, AUTHENTICATION AND SERVICES.....	34
4.1	ROLES	34
4.1.1	<i>Crypto Officer Authentication</i>	35
4.1.2	<i>User Authentication</i>	35
4.1.3	<i>Wireless Client Authentication</i>	35
4.1.4	<i>Strength of Authentication Mechanisms</i>	36
4.2	SERVICES.....	37
4.2.1	<i>Crypto Officer Services</i>	37
4.2.2	<i>User Services</i>	38
4.2.3	<i>Wireless Client Services</i>	39
4.2.4	<i>Unauthenticated Services</i>	39
4.2.5	<i>Services Available in Non-FIPS Mode</i>	39
4.2.6	<i>Non-Approved Services Disallowed in FIPS Mode</i>	39
5	CRYPTOGRAPHIC ALGORITHMS	40
6	CRITICAL SECURITY PARAMETERS.....	44
7	SELF-TESTS	50
8	SECURE OPERATION.....	52
8.1	VERIFY THAT THE MODULE IS IN FIPS MODE.....	52
8.2	FULL DOCUMENTATION	52
8.3	DISALLOWED FIPS MODE CONFIGURATIONS	53

1 Introduction

This document constitutes the non-proprietary Cryptographic Module Security Policy for the Aruba AP-304, AP-305, AP-314, AP-315, AP-334, AP-335, AP-365, and AP-367 Wireless Access Points with FIPS 140-2 Level 2 validation from Aruba Networks. This security policy describes how the AP meets the security requirements of FIPS 140-2 Level 2, and how to place and maintain the AP in a secure FIPS 140-2 mode. This policy was prepared as part of the FIPS 140-2 Level 2 validation of the product.

FIPS 140-2 (Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*) details the U.S. Government requirements for cryptographic modules. More information about the FIPS 140-2 standard and validation program is available on the National Institute of Standards and Technology (NIST) Web-site at:

<https://csrc.nist.gov/projects/cryptographic-module-validation-program>

This document can be freely distributed.

- The exact firmware version: ArubaOS 8.5.0.3-FIPS and ArubaOS 8.2.2.5-FIPS

The functionality provided under ArubaOS 8.5 and 8.2 meets the requirements for CMVP testing for FIPS 140-2 and future releases under AOS 8.5 and 8.2 will maintain compliance to the claims made within this document. The CMVP makes no claim as to the correct operation of the module or the security strengths of the generated keys when ported to an operational environment which is not listed on the validation certificate.

In addition, in this document, the Aruba AP-304, AP-305, AP-314, AP-315, AP-334, AP-335, AP-365 and AP-367 Wireless Access Points are referred to as the Access Point, the AP, the module, the cryptographic module, and Aruba Wireless AP.

1.1 Acronyms and Abbreviations

AES	Advanced Encryption Standard
AP	Access Point
CBC	Cipher Block Chaining
CLI	Command Line Interface
CO	Crypto Officer
CPSec	Control Plane Security protected
CSEC	Communications Security Establishment Canada
CSP	Critical Security Parameter
ECO	External Crypto Officer
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
FE	Fast Ethernet
GE	Gigabit Ethernet
GHz	Gigahertz
HMAC	Hashed Message Authentication Code
Hz	Hertz
IKE	Internet Key Exchange
IPsec	Internet Protocol security
KAT	Known Answer Test
KEK	Key Encryption Key
L2TP	Layer-2 Tunneling Protocol
LAN	Local Area Network
LED	Light Emitting Diode
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SPOE	Serial & Power Over Ethernet
TEL	Tamper-Evident Label
TFTP	Trivial File Transfer Protocol
WLAN	Wireless Local Area Network

2 Product Overview

This section introduces the various Aruba Wireless Access Points, providing a brief overview and summary of the physical features of each model covered by this FIPS 140-2 security policy.

The tested version of the firmware is: **ArubaOS 8.5.0.3-FIPS and ArubaOS 8.2.2.5-FIPS**

Aruba's development processes are such that future releases under AOS 8.2 and 8.5 should be FIPS validate-able and meet the claims made in this document. Only the versions that explicitly appear on the certificate, however, are formally validated. The CMVP makes no claim as to the correct operation of the module or the security strengths of the generated keys when operating under a version that is not listed on the validation certificate.

2.1 AP-304

This section introduces the various Aruba Wireless Access Points, providing a brief overview and summary of the physical features of each model covered by this FIPS 140-2 security policy.



Figure 1 - Aruba AP-304

This section introduces the Aruba AP-304 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

These compact and cost-effective dual-radio APs implement a dual radio 802.11ac Access Point with Multi-User MIMO - Supports up to 1,300 Mbps in the 5GHz band (with 3SS/ VHT80 clients) and up to 400 Mbps in the 2.4GHz band (with 2SS/VHT40 clients).

When managed by Aruba Mobility Controllers, AP-304 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.1.1 Physical Description

The Aruba AP-304 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through three N-type female connectors for external antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: AP-304-F1 (HPE SKU JX937A)

2.1.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (unit, excluding mount accessories): - 165mm x 165mm x 38mm - 460g

Environmental:

- Operating: - Temperature: 0° C to +50° C (+32° F to +122° F) - Humidity: 5% to 95% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

2.1.1.2 Interfaces

The module provides the following network interfaces:

- 1 - 10/100/1000BASE-T Ethernet network interface (RJ-45)
- Serial Console port (proprietary; optional adapter cable available; disabled in FIPS mode)
- USB 2.0 Host Interface
- PoE-PD: 48 Vdc (nominal) 802.3af or 802.3at PoE

DC power interface, accepts 2.1/5.5-mm center-positive

- 12V DC power interface circular plug with 9.5-mm length

Bluetooth Low Energy (BLE) radio

- Up to 4dBm transmit power (class 2) and -94dBm receive sensitivity

Other Interfaces

- Visual indicators (tri-color LEDs): For system and radio status
- Reset button: Factory reset (during device power up)

LED	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green- Solid	Device ready
	Amber- Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Restricted mode: * Uplink negotiated in sub optimal speed; or

Radio Status (Right)		* Radio in non-high throughput (HT) mode
	Red	System error condition
	Off	AP powered off, or both radios disabled
	Green- Solid	Both radios enabled in access mode
	Amber- Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	One radio enabled in access mode, one enabled in monitor mode

Table 1 - AP-304 LED Status Indicators

2.2 AP-305



Figure 2 - Aruba AP-305

This section introduces the Aruba AP-305 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

These compact and cost-effective dual-radio APs implement a dual radio 802.11ac Access Point with Multi-User MIMO - Supports up to 1,300 Mbps in the 5GHz band (with 3SS/ VHT80 clients) and up to 400 Mbps in the 2.4GHz band (with 2SS/VHT40 clients).

When managed by Aruba Mobility Controllers, AP-305 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.2.1 Physical Description

The Aruba AP-305 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports internal antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: AP-305-F1(HPE SKU JX938A)

2.2.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (unit, excluding mount accessories): - 165mm x 165mm x 38mm - 460g

Environmental:

- Operating: - Temperature: 0° C to +50° C (+32° F to +122° F) - Humidity: 5% to 95% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

2.2.1.2 Interfaces

The module provides the following network interfaces:

- 1 - 10/100/1000BASE-T Ethernet network interface (RJ-45)
- Serial Console port (proprietary; optional adapter cable available; disabled in FIPS mode)
- USB 2.0 Host Interface
- PoE-PD: 48 Vdc (nominal) 802.3af or 802.3at PoE

DC power interface, accepts 2.1/5.5-mm center-positive

- 12V DC power interface circular plug with 9.5-mm length

Bluetooth Low Energy (BLE) radio

- Up to 4dBm transmit power (class 2) and -94dBm receive sensitivity

Other Interfaces

- Visual indicators (tri-color LEDs): For system and radio status
- Reset button: Factory reset (during device power up)

LED	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green- Solid	Device ready
	Amber- Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition

Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green- Solid	Both radios enabled in access mode
	Amber- Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	One radio enabled in access mode, one enabled in monitor mode

Table 2 - AP-305 LED Status Indicators

2.3 AP-314



Figure 3 - Aruba AP-314

This section introduces the Aruba AP-314 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

These compact and cost-effective dual-radio APs implement a dual radio 802.11ac access point with Multi-User MIMO - Supports up to 1,733Mbps in the 5GHz band (with 4SS/VHT80 or 2SS/VHT160 clients) and up to 300 Mbps in the 2.4 GHz band (with 2SS/VHT40 clients).

When managed by Aruba Mobility Controllers, AP-314 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.3.1 Physical Description

The Aruba AP-314 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through four N-type female connectors for external antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: AP-314-F1 (HPE SKU JW796A)

2.3.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (unit, excluding mount accessories): - 182mm (W) x 180mm (D) x 48mm (H) - 650g/23oz
- Dimensions/weight (shipping): - 223mm (W) x 218mm (D) x 55mm (H) - 850g/30oz

Environmental

- Operating: - Temperature: 0° C to +50° C (+32° F to +122° F) - Humidity: 5% to 93% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

2.3.1.2 Interfaces

The module provides the following network interfaces:

- One 0/100/1000BASE-T Ethernet network interfaces (RJ-45)
- Auto-sensing link speed and MDI/MDX
- Link Aggregation support to achieve platform throughput up to 2 Gbps
- 802.3az Energy Efficient Ethernet (EEE)
- PoE-PD: 48 Vdc (nominal) 802.3af or 802.3at PoE

DC power interface, accepts 2.1/5.5-mm center-positive

- 12V DC power interface circular plug with 9.5-mm length
- USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio

- Up to 4dBm transmit power (class 2) and -91dBm receive sensitivity

Other Interfaces

- Visual indicators (tri-color LEDs): For system and radio status
- Reset button: Factory reset (during device power up)
- Serial console interface (proprietary; optional adapter cable available; disabled in FIPS mode)

LED	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green- Solid	Device ready
	Amber- Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode

	Red	System error condition
Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green- Solid	Both radios enabled in access mode
	Amber- Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	One radio enabled in access mode, one enabled in monitor mode

Table 3 - AP-314 LED Status Indicators

2.4 AP-315



Figure 4 - Aruba AP-315

This section introduces the Aruba AP-315 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

These compact and cost-effective dual-radio APs deliver wireless data rates of up to 1,733Mbps in the 5GHz band (with 4SS/VHT80 or 2SS/VHT160 clients) and up to 300 Mbps in the 2.4 GHz band (with 2SS/HT40 clients).

When managed by Aruba Mobility Controllers, AP-315 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.4.1 Physical Description

The Aruba AP-315 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through four internal antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: AP-315-F1(HPE SKU JW798A)

2.4.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (unit, excluding mount accessories): - 182mm (W) x 180mm (D) x 48mm (H) - 650g/23oz
- Dimensions/weight (shipping 223mm (W) x 218mm (D) x 55mm (H) - 850g/30oz

Environmental

- Operating: - Temperature: 0° C to +50° C (+32° F to +122° F) - Humidity: 5% to 95% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

2.4.1.2 Interfaces

The module provides the following network interfaces:

- One 10/100/1000BASE-T Ethernet network interfaces (RJ-45)
- Auto-sensing link speed and MDI/MDX
- Link Aggregation support to achieve platform throughput up to 2 Gbps
- 802.3az Energy Efficient Ethernet (EEE)
- PoE-PD: 48 Vdc (nominal) 802.3af or 802.3at PoE

DC power interface, accepts 2.1/5.5-mm center-positive

- 12V DC power interface circular plug with 9.5-mm length
- USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio

- Up to 4dBm transmit power (class 2) and -91Bm receive sensitivity

Other Interfaces

- Visual indicators (tri-color LEDs): For system and radio status
- Reset button: Factory reset (during device power up)
- Serial console interface (proprietary; optional adapter cable available; disabled in FIPS mode)

LED	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green- Solid	Device ready
	Amber- Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition

Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green- Solid	Both radios enabled in access mode
	Amber- Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	One radio enabled in access mode, one enabled in monitor mode

Table 4 - AP-315 LED Status Indicators

2.5 AP-334



Figure 5 - Aruba AP-334

This section introduces the Aruba AP-334 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

With a maximum concurrent data rate of 1,733 Mbps in the 5 GHz band and 600 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.3Gbps), the 330 Series Access Points deliver a best-in-class, next-generation 802.11ac Wi-Fi infrastructure that is ideal for lecture halls, auditoriums, public venues, and high-density office environments. The high performance and high density 802.11ac 330 Series Access Points support 160 MHz channel bandwidth (VHT160), 4-stream multi-user MIMO (MU-MIMO) and 4 spatial streams (4SS). Four RP-SMA connectors for external dual band antennas. Internal loss between radio interface and external antenna connectors (due to diplexing circuitry): 2.3 dB in 2.4 GHz and 1.2 dB in 5 GHz

When managed by Aruba Mobility Controllers, AP-334 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.5.1 Physical Description

The Aruba AP-334 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports external antennas through four N-type female connectors for external antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: AP-334-F1 (HPE SKU JW800A)

2.5.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (unit, excluding mount accessories): - - 225mm (W) x 224mm (D) x 52mm (H) 8.9" (W) x 8.9" (D) x 2.0" (H) - 1150g/41oz
- Dimensions/weight (shipping): - 335mm (W) x 290mm (D) x 85mm (H) 13.2" (W) x 11.4" (D) x 3.35" (H) - 1750g/62oz

Environmental

- Operating: - Temperature: 0° C to +50° C (+32° F to +122° F) - Humidity: 5% to 95% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

2.5.1.2 Interfaces

The module provides the following network interfaces:

- One HPE Smart Rate port (RJ-45, Auto-sensing link speed 100/1000/2500/5000BASE-T)
- One 10/100/1000BASE-T Ethernet network interfaces (RJ-45)
- Auto-sensing link speed and MDI/MDX
- Link Aggregation support to achieve platform throughput up to 2 Gbps
- 802.3az Energy Efficient Ethernet (EEE)
- PoE-PD: 48 Vdc (nominal) 802.3af or 802.3at PoE

DC power interface, 48Vdc nominal, +/- 5%

- 1.35/3.5-mm center-positive circular plug with 9.5-mm length

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio

- Up to 4dBm transmit power (class 2) and -91dBm receive sensitivity

Other Interfaces

- Visual indicators (tri-color LEDs): For system and radio status
- Reset button: Factory reset (during device power up)
- Serial console interface (proprietary; optional adapter cable available; disabled in FIPS mode)

LED	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green- Solid	Device ready
	Amber- Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition
Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green- Solid	Both radios enabled in access mode
	Amber- Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	One radio enabled in access mode, one enabled in monitor mode

Table 5 - AP-334 LED Status Indicators

2.6 AP-335



Figure 6 - Aruba AP-335

This section introduces the Aruba AP-335 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

With a maximum concurrent data rate of 1,733 Mbps in the 5 GHz band and 600 Mbps in the 2.4 GHz band (for an aggregate peak data rate of 2.3Gbps), the 330 Series Access Points deliver a best-in-class, next-generation 802.11ac Wi-Fi infrastructure that is ideal for lecture halls, auditoriums, public venues, and high-density office environments. The high performance and high density 802.11ac 330 Series Access Points support 160 MHz channel bandwidth (VHT160), 4-stream multi-user MIMO (MU-MIMO) and 4 spatial streams (4SS). The AP has a total of twelve integrated omni-directional downtilt antennas.

Four (vertically polarized) integrated 2.4 GHz downtilt omni-directional antennas for 4x4 MIMO with peak antenna gain of 4.3 dBi per antenna. - Each 5 GHz radio chain has both a vertically and a horizontally polarized antenna element; AP software automatically and dynamically selects the best set of elements for each data packet transmitted or received. - Four integrated vertically polarized 5 GHz downtilt omnidirectional antennas for 4x4 MIMO with peak antenna gain of 5.4 dBi per antenna - Four integrated horizontally polarized 5 GHz downtilt omni-directional antennas for 4x4 MIMO with peak antenna gain of 4.2 dBi per antenna - Built-in antennas are optimized for horizontal ceiling mounted orientation of the AP. The downtilt angle for maximum gain is roughly 30 degrees. - Combining the patterns of each of the antennas of the MIMO radios, the peak gain of the effective per-antenna pattern is 2.6dBi in 2.4 GHz and 2.5 dBi (vertical) or 2.1 dB (horizontal) in 5 GHz.

When managed by Aruba Mobility Controllers, AP-335 offers centralized configuration, data encryption, policy enforcement and network services, as well as distributed and centralized traffic forwarding.

2.6.1 Physical Description

The Aruba AP-335 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports twelve integrated omni-directional downtilt antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: AP-335-F1(HPE SKU JW802A)

2.6.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (unit, excluding mount accessories): - 203mm (W) x 203mm (D) x 57mm (H) 8.0" (W) x 8.0" (D) x 2.2" (H) - 950g/34 oz
- Dimensions/weight (shipping): - 335mm (W) x 290mm (D) x 85mm (H) 13.2" (W) x 11.4" (D) x 3.35" (H) - 1750g/62oz

Environmental

- Operating: - Temperature: 0° C to +50° C (+32° F to +122° F) - Humidity: 5% to 95% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

2.6.1.2 Interfaces

The module provides the following network interfaces:

- One HPE Smart Rate port (RJ-45, Auto-sensing link speed 100/1000/2500/5000BASE-T)
- One 10/100/1000BASE-T Ethernet network interfaces (RJ-45)
- Auto-sensing link speed and MDI/MDX
- Link Aggregation support to achieve platform throughput up to 2 Gbps
- 802.3az Energy Efficient Ethernet (EEE)
- PoE-PD: 48 Vdc (nominal) 802.3af or 802.3at PoE

DC power interface, 48Vdc nominal, +/- 5%

- 1.35/3.5-mm center-positive circular plug with 9.5-mm length

USB 2.0 host interface (Type A connector)

Bluetooth Low Energy (BLE) radio

- Up to 4dBm transmit power (class 2) and -91dBm receive sensitivity

Other Interfaces

- Visual indicators (tri-color LEDs): For system and radio status
- Reset button: Factory reset (during device power up)
- Serial console interface (proprietary; optional adapter cable available; disabled in FIPS mode)

LED	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Green/Amber Alternating	Device booting; not ready
	Green- Solid	Device ready
	Amber- Solid	Device ready; power-save mode (802.3af PoE): * Single radio * USB disabled
	Green or Amber Flashing	Restricted mode: * Uplink negotiated in sub optimal speed; or * Radio in non-high throughput (HT) mode
	Red	System error condition

Radio Status (Right)	Off	AP powered off, or both radios disabled
	Green- Solid	Both radios enabled in access mode
	Amber- Solid	Both radios enabled in monitor mode
	Green/Amber Alternating	One radio enabled in access mode, one enabled in monitor mode

Table 6 - AP-335 Status Indicators

2.7 AP-365



Figure 7 - Aruba AP-365

This section introduces the Aruba AP-365 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

By supporting dual radio operation, the 360 Series APs deliver a maximum data rate of 867 Mbps in the 5-GHz band and 400 Mbps in the 2.4-GHz band, while supporting MU-MIMO operation for simultaneous transmission for up to two 802.11ac Wave 2 devices.

Able to survive in harsh outdoor environments, the 360 Series can withstand exposure to high and low temperatures, persistent moisture and precipitation, and are fully sealed to keep out airborne contaminants. All electrical interfaces include industrial strength surge protection.

The outdoor 360 Series have integrated Aruba ClientMatch™ technology to eliminate sticky clients and enhanced Wave 2 WLAN performance. These outdoor APs continuously gather session performance metrics and utilize the data to steer mobile devices to the best AP and radio on the WLAN, even while users roam. The enhanced ClientMatch technology enables the 360 Series to automatically detect, classify and group 802.11ac Wave 2 capable mobile devices under a single Wave 2 radio, increasing network capacity and efficiency.

2.7.1 Physical Description

The Aruba AP-365 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports internal omnidirectional antennas.

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: Aruba AP-365-F1 (US) FIPS/TAA (HPE SKU JX969A)

2.7.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (unit, excluding mount accessories): 165mm (W) x 165mm (D) x 110mm (H), 6.5" (W) x 6.5" (D) 4.3" (H)/ 807g/1.78lbs
- Environmental: Operating: - Temperature: -40° C to +55° C (-40° F to +131° F) - Humidity: 5% to 95% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

2.7.1.2 Interfaces

The module provides the following network interfaces:

- One 10/100/1000BASE-T Ethernet network interfaces (RJ-45)
 - Auto-sensing link speed and MDI/MDX
 - 802.3az Energy Efficient Ethernet (EEE)
 - PoE-PD: 48 VDC (nominal) 802.3af or 802.3at PoE
- Bluetooth Low Energy (BLE) radio

Other Interfaces

- Visual indicators (tri-color LEDs): For system and radio status
- Reset button: Factory reset (during device power up)
- Serial console interface (Micro USB – Proprietary pinout)

LED	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Red	Initial Power-Up
	Green Flashing	Device booting;
	Green - Solid	Device ready, 1000 Mbps, light goes out after 1200 seconds
	Green – Yellow, Flashing 6 seconds	Device ready, 10/100 Mbps, light goes out after 1200 seconds
	Red	General fault
	Red, one blink off every 3 seconds	Radio 0 fault (5 GHz)
	Red, two quick blinks off (0.5 sec apart) every 3 seconds	Radio 1 fault (2.4 GHz)

Table 7 - AP-365 LED Status Indicators

2.8 AP-367



Figure 8 - Aruba AP-367

This section introduces the Aruba AP-367 Wireless Access Point (AP) with FIPS 140-2 Level 2 validation. It describes the purpose of the AP, its physical attributes, and its interfaces.

By supporting dual radio operation, the 360 Series APs deliver a maximum data rate of 867 Mbps in the 5-GHz band and 400 Mbps in the 2.4-GHz band, while supporting MU-MIMO operation for simultaneous transmission for up to two 802.11ac Wave 2 devices.

Able to survive in harsh outdoor environments, the 360 Series can withstand exposure to high and low temperatures, persistent moisture and precipitation, and are fully sealed to keep out airborne contaminants. All electrical interfaces include industrial strength surge protection.

The outdoor 360 Series have integrated Aruba ClientMatch™ technology to eliminate sticky clients and enhanced Wave 2 WLAN performance. These outdoor APs continuously gather session performance metrics and utilize the data to steer mobile devices to the best AP and radio on the WLAN, even while users roam. The enhanced ClientMatch technology enables the 360 Series to automatically detect, classify and group 802.11ac Wave 2 capable mobile devices under a single Wave 2 radio, increasing network capacity and efficiency.

2.8.1 Physical Description

The Aruba AP-367 Access Point is a multi-chip standalone cryptographic module consisting of hardware and software, all contained in a hard, opaque plastic case. The module contains 802.11 a/b/g/n/ac transceivers and supports internal directional antennas..

The case physically encloses the complete set of hardware and software components and represents the cryptographic boundary of the module.

The Access Point configuration validated during the cryptographic module testing included:

- HW: Aruba AP-367-F1 (US) FIPS/TAA (HPE SKU JX976A)

2.8.1.1 Dimensions/Weight

The AP has the following physical dimensions:

- Dimensions/weight (unit, excluding mount accessories): 165mm (W) x 165mm (D) x 110mm (H), 6.5" (W) x 6.5" (D) 4.3" (H)/ 807g/1.78lbs
- Environmental: Operating: - Temperature: -40° C to +55° C (-40° F to +131° F) - Humidity: 5% to 95% non-condensing

Storage and transportation:

- Temperature: -40° C to +70° C (-40° F to +158° F)

2.8.1.2 Interfaces

The module provides the following network interfaces:

- One 10/100/1000BASE-T Ethernet network interfaces (RJ-45)
 - Auto-sensing link speed and MDI/MDX
 - 802.3az Energy Efficient Ethernet (EEE)
 - PoE-PD: 48 VDC (nominal) 802.3af or 802.3at PoE
- Bluetooth Low Energy (BLE) radio

Other Interfaces

- Visual indicators (tri-color LEDs): For system and radio status
- Reset button: Factory reset (during device power up)
- Serial console interface (Micro USB – Proprietary pinout)

LED	Color/State	Meaning
System Status (Left)	Off	AP powered off
	Red	Initial Power-Up
	Green Flashing	Device booting;
	Green - Solid	Device ready, 1000 Mbps, light goes out after 1200 seconds
	Green – Yellow, Flashing 6 seconds	Device ready, 10/100 Mbps, light goes out after 1200 seconds
	Red	General fault
	Red, one blink off every 3 seconds	Radio 0 fault (5 GHz)
	Red, two quick blinks off (0.5 sec apart) every 3 seconds	Radio 1 fault (2.4 GHz)

Table 8 - AP-367 LED Status Indicators

3 Module Objectives

This section describes the assurance levels for each of the areas described in the FIPS 140-2 Standard.

3.1 Security Levels

Section	Section Title	Level
1	Cryptographic Module Specification	2
2	Cryptographic Module Ports and Interfaces	2
3	Roles, Services, and Authentication	2
4	Finite State Model	2
5	Physical Security	2
6	Operational Environment	N/A
7	Cryptographic Key Management	2
8	EMI/EMC	2
9	Self-tests	2
10	Design Assurance	2
11	Mitigation of Other Attacks	N/A
Overall	Overall module validation level	2

Table 9 - Security Levels

3.2 Physical Security

The Aruba Wireless AP is a scalable, multi-processor standalone network device and is enclosed in a hard, opaque plastic case. The AP enclosure is resistant to probing (please note that this feature has not been validated as part of the FIPS 140-2 validation) and is opaque within the visible spectrum. The enclosure of the AP has been designed to satisfy FIPS 140-2 Level 2 physical security requirements.

3.2.1 Applying TELs

The Crypto Officer must apply Tamper-Evident Labels (TELs) to the AP to allow detection of the opening of the device, and to block the serial console port (on the bottom of the device). The TELs shall be installed for the module to operate in a FIPS Approved mode of operation. Vendor provides FIPS 140 designated TELs which have met the physical security testing requirements for tamper evident labels under the FIPS 140-2 Standard. TELs are not endorsed by the Cryptographic Module Validation Program (CMVP). Aruba provides double the required amount of TELs with shipping and additional replacement TELs can be obtained by calling customer support and requesting part number 4011570-01 (HPE SKU JY894A).

The Crypto Officer is responsible for securing and having control at all times of any unused tamper evident labels. If evidence of tampering is found with the TELs, the module must immediately be powered down and the administrator must be made aware of a physical security breach. The Crypto Officer should employ TELs as follows:

- Before applying a TEL, make sure to clean the target surfaces with alcohol and let dry.
- Do not cut, trim, punch, or otherwise alter the TEL.
- Apply the wholly intact TEL firmly and completely to the target surfaces.
- Ensure that TEL placement is not defeated by simultaneous removal of multiple modules.
- Allow 24 hours for the TEL adhesive seal to completely cure.
- Record the position and serial number of each applied TEL in a security log.
- To obtain additional or replacement TELS, please order Aruba Networks part number: 4011570—01 (HPE SKU JY894A).

Once applied, the TELs included with the AP cannot be surreptitiously broken, removed or reapplied without an obvious change in appearance:



Each TEL has a unique serial number to prevent replacement with similar label. To protect the device from tampering, TELs should be applied by the Crypto Officer as pictured below:

3.2.2 TELs Placement

This section displays all the TELs locations on each of module.

3.2.2.1 TELs Placement on the AP-304

The AP-304s requires 3 TELs. One on each side edge (labels 1 and 2) and one covering the console port (label 3). See figures 9 and 10 for placement.



Figure 9 - Top View of AP-304 with TELs



Figure 10 – Bottom View of AP-304 with TELs

3.2.2.2 TELs Placement on the AP-305

The AP-305 require 3 TELs. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 11 and 12 for placement.



Figure 11 – Top View of AP-305 with TELs



Figure 12 – Bottom View of AP-305 with TELs

3.2.2.3 TELs Placement on the AP-314

The AP-314 requires three TELs. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 13 and 14 for placement.



Figure 13 - Top View of AP-314 with TELs



Figure 14 – Bottom View of AP-314 with TELs

3.2.2.4 TELs Placement on the AP-315

The AP-315s require 3 TELs. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 15 and 16 for placement.



Figure 15 – Top View of AP-315 with TELs



Figure 16 – Bottom View of AP-315 with TELs

3.2.2.5 TELs Placement on the AP-334

The AP-334s requires three TELs. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 17 and 18 for placement.



Figure 17 - Top View of AP-334 with TELs



Figure 18 – Bottom View of AP-334 with TELs

3.2.2.6 TELs Placement on the AP-335

The AP-335s require 3 TELs. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 19 and 20 for placement.



Figure 19 – Top View of AP-335 with TELs



Figure 20 – Bottom View of AP-335 with TELs

3.2.2.7 TELs Placement on the AP-365

The AP-365s require 3 TELs. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 21 and 22 for placement.



Figure 21 – Top View of AP-365 with TELs



Figure 22 – Bottom View of AP-365 with TELs

3.2.2.8 TELs Placement on the AP-367

The AP-367s require 3 TELs. One on each edge (labels 1 and 2) and one covering the console port (label 3). See figures 23 and 24 for placement.



Figure 23 – Top View of AP-367 with TELs

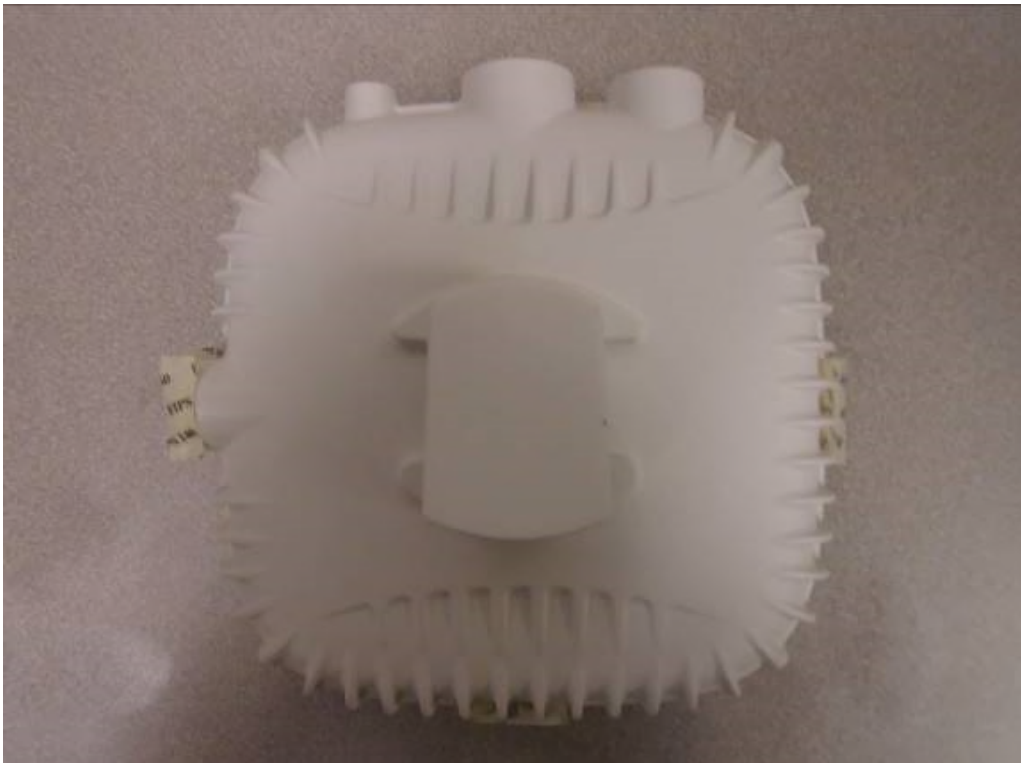


Figure 24 – Bottom View of AP-367 with TELs

3.2.3 Inspection/Testing of Physical Security Mechanisms

Physical Security Mechanism	Recommended Test Frequency	Guidance
Tamper-evident labels (TELS)	Once per month	Examine for any sign of removal, replacement, tearing, etc. See images above for locations of TELS. If any TELS are found to be missing or damaged, contact a system administrator immediately.
Opaque module enclosure	Once per month	Examine module enclosure for any evidence of new openings or other access to the module internals. If any indication is found that indicates tampering, contact a system administrator immediately.

Table 10 - Inspection/Testing of Physical Security Mechanisms

3.3 Operational Environment

The FIPS 140-2 Operational Environment requirements are not applicable because the module is designated as a non-modifiable operational environment. The module only allows the loading of trusted and verified firmware that is signed by Aruba.

3.4 Logical Interfaces

The physical interfaces are divided into logical interfaces defined by FIPS 140-2 as described in the following table.

FIPS 140-2 Logical Interface	Module Physical Interface
Data Input Interface	<ul style="list-style-type: none">• 10/100/1000 Ethernet Ports• 802.11a/b/g/n/ac Antenna Interfaces
Data Output Interface	<ul style="list-style-type: none">• 10/100/1000 Ethernet Ports• 802.11a/b/g/n/ac Antenna Interfaces
Control Input Interface	<ul style="list-style-type: none">• 10/100/1000 Ethernet Ports• 802.11a/b/g/n/ac Antenna Interfaces• Reset button
Status Output Interface	<ul style="list-style-type: none">• 10/100/1000 Ethernet Ports• 802.11a/b/g/n/ac Antenna Interfaces• LED Status Indicators
Power Interface	<ul style="list-style-type: none">• Power Input• Power-over-Ethernet (POE)

Table 11 - Logical Interfaces

Data input and output, control input, status output, and power interfaces are defined as follows:

- Data input and output are the packets that use the networking functionality of the module.
- Control input consists of manual control inputs for power and reset through the power interfaces (power supply or POE). It also consists of all of the data that is entered into the access point while using the management interfaces. A reset button is present which is used to reset the AP to factory default settings.
- Status output consists of the status indicators displayed through the LEDs, the status data that is output from the module while using the management interfaces, and the log file.
 - LEDs indicate the physical state of the module, such as power-up (or rebooting), utilization level, and activation state. The log file records the results of self-tests, configuration errors, and monitoring data.
- The module may be powered by an external power supply. Operating power may also be provided via Power Over Ethernet (POE) device, when connected, the power is provided through the connected Ethernet cable.
- Console port is disabled when operating in FIPS mode by TEL.

The module distinguishes between different forms of data, control, and status traffic over the network ports by analyzing the packet headers and contents.

4 Roles, Authentication and Services

4.1 Roles

The module supports the role-based authentication of Crypto Officer, User, and Wireless Client; no additional roles (e.g., Maintenance) are supported. Administrative operations carried out by the Aruba Mobility Controller or Aruba Mobility Master map to the Crypto Officer role. The Crypto Officer has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs. Configuration can be performed through a standalone Mobility Controller or by a Mobility Master if deployed in the environment. The Mobility master also acts as a CO for the APs.

Defining characteristics of the roles depend on whether the module is configured as in either Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode or Mesh AP FIPS Mode. There are four FIPS approved modes of operations, which are Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode and the two Mesh Modes, Mesh Portal FIPS Mode and Mesh Point FIPS Mode. Please refer to section 8 in this documentation for more information.

- **Remote AP FIPS mode:**
 - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
 - User role: in the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer role.
 - Wireless Client role: in Remote AP FIPS mode configuration, a wireless client can create a connection to the module using 802.11i and access wireless network access/bridging services. When Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via 802.11i Pre-shared secret only.
- **CPSec Protected AP FIPS mode:**
 - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
 - User role: in the configuration, the User operator shares the same services and authentication techniques as the Mobility Controller in the Crypto Officer
 - Wireless Client role: in CPSec Protected AP FIPS mode configuration, a wireless client can create a connection to the module using 802.11i Pre-shared secret and access wireless network access services.
- **Mesh Portal FIPS mode:**
 - Crypto Officer role: the Crypto Officer is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs.
 - User role: the adjacent Mesh Point APs in a given mesh cluster. Please notice that Remote Mesh Portal AP must be physically wired to Mobility Controller.
 - Wireless Client role: in Mesh Portal FIPS AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.

- **Mesh Point FIPS mode:**
 - Crypto Officer role: the Crypto Officer role is the Aruba Mobility Controller or Mobility Master that has the ability to configure, manage, and monitor the module, including the configuration, loading, and zeroization of CSPs. The first mesh AP configured is the only AP with the direct wired connection.
 - User role: the adjacent Mesh APs in a given mesh cluster. Please notice that User role can be a Mesh Point AP or a Mesh Portal AP in the given mesh network.
 - Wireless Client role: in Mesh Mesh Point FIPS AP configuration, a wireless client can create a connection to the module using WPA2 and access wireless network access services.

4.1.1 Crypto Officer Authentication

In each of FIPS approved modes, the Aruba Mobility Controller or Mobility Master implements the Crypto Officer role. Connections between the module and the mobility controller are protected using IPsec. Crypto Officer's authentication is accomplished via either Pre-shared secret (IKEv1), RSA digital certificate (IKEv1/IKEv2) or ECDSA digital certificate (IKEv2). The Mobility Master interacts with the APs through the Mobility Controller through provisioning of configurations.

4.1.2 User Authentication

Authentication for the User role depends on the module configuration. When the module is configured in Mesh Portal FIPS mode or Mesh Point FIPS mode, the User role is authenticated via the WPA2 pre-shared key or EAP. When the module is configured as a Remote AP FIPS mode and CPsec protected AP FIPS mode, the User role is authenticated via the same IKEv1/IKEv2 pre-shared key or RSA/ECDSA certificate that is used by the Crypto Officer.

4.1.3 Wireless Client Authentication

The wireless client role defined in each of FIPS approved modes authenticates to the module via 802.11i. Please notice that WEP and TKIP configurations are not permitted in FIPS mode. When Remote AP cannot communicate with the controller, the wireless client role authenticates to the module via 802.11i Pre-shared secret only.

4.1.4 Strength of Authentication Mechanisms

The following table describes the relative strength of each supported authentication mechanism.

Authentication Mechanism	Mechanism Strength
IKEv1 Pre-shared secret based authentication (CO/User role)	<p>Passwords are required to be a minimum of eight ASCII characters and a maximum of 64 with a minimum of one letter and one number, or 64 HEX characters. Assuming the weakest option of 8 ASCII characters with the listed restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it is double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/3,608,347,333,959,680$, which is less than 1 in 100,000 required by FIPS 140-2.</p>
802.11i Pre-shared secret based authentication (Wireless Client and Mesh AP user roles)	<p>Passwords are required to be a minimum of eight ASCII characters and a maximum of 63 with a minimum of one letter and one number, or the password must be exactly 64 HEX characters. Assuming the weakest option of 8 ASCII characters with the listed restrictions, the probability of randomly guessing the correct sequence is one (1) in 3,608,347,333,959,680 (this calculation is based on the assumption that the typical standard American QWERTY computer keyboard has 10 Integer digits, 52 alphabetic characters, and 32 special characters providing 94 characters to choose from in total. The calculation should be 94^8 (Total number of 8-digit passwords) – 84^8 (Total number of 8-digit passwords without numbers) – 42^8 (Total number of 8-digit passwords without letters) + 32^8 (Total number of 8-digit passwords without letters or numbers, added since it is double-counted in the previous two subtractions) = 3,608,347,333,959,680). At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/3,608,347,333,959,680$, which is less than 1 in 100,000 required by FIPS 140-2.</p>
RSA Certificate based authentication (CO/User role)	<p>The module supports 2048-bit RSA key authentication during IKEv1 and IKEv2. RSA 2048 bit keys correspond to 112 bits of security. Assuming the low end of that range, the associated probability of a successful random attempt is 1 in 2^{112}, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/2^{112}$, which is less than 1 in 100,000 required by FIPS 140-2.</p>
ECDSA Certificate based authentication (CO/User role)	<p>ECDSA signing and verification is used to authenticate to the module during IKEv1/IKEv2. Both P-256 and P-384 curves are supported. ECDSA P-256 provides 128 bits of equivalent security, and P-384 provides 192 bits of equivalent security. Assuming the low end of that range, the associated probability of a successful random attempt during a one-minute period is 1 in 2^{128}, which is less than 1 in 1,000,000 required by FIPS 140-2. At optimal network conditions (assuming 1ms round-trip latency), an attacker would only get 60,000 guesses per minute. Therefore the associated probability of a successful random attempt during a one-minute period is $60,000/2^{128}$, which is less than 1 in 100,000 required by FIPS 140-2.</p>

Table 12 - Strength of Authentication Mechanisms

4.2 Services

The module provides various services depending on role. These are described below.

4.2.1 Crypto Officer Services

The CO role in each of FIPS modes defined in section 4.1 has the same services.

Services	Description	CSPs Accessed (see section 6 below for a complete description to each CSP and the associated cryptographic algorithms)
FIPS mode enable/disable	The CO enables FIPS mode by following the procedures under Section 8 to ensure the AP is configured for Secure Operations. The CO can disable FIPS mode by reverting these changes.	None.
Key Management	The CO can configure/modify the IKEv1/IKEv2 shared secret (The RSA private key is protected by non-volatile memory and cannot be modified), IKEv1/IKEv2 certifications, and the 802.11i Pre-shared secret (used in advanced Remote AP configuration). Also, the CO/User implicitly uses the KEK to read/write configuration to non-volatile memory.	1 (read), 13 and 25(write)
Remotely reboot module	The CO can remotely trigger a reboot	None
Self-test triggered by CO/User reboot	The CO can trigger a programmatic reset leading to self-test and initialization	None.
Update module firmware ¹	The CO can trigger a module firmware update	1, 12 (read)
Configure non-security related module parameters	CO can configure various operational parameters that do not relate to security	None.
Creation/use of secure management session between module and CO ²	The module supports use of IPSec for securing the management channel.	2, 3, 4, 5, 6, 7, 8, 9, 10, 11 (read, write) 13 (read) 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24 (read, write)
System Status	CO may view system status information through the secured management channel	See creation/use of secure management session above.

¹ Any firmware loaded into this module that is not shown on the module certificate is out of the scope of this validation and requires a separate FIPS 140-2 validation.

² This service is not available in Mesh Point FIPS mode. In Mesh Point mode, the IPSec tunnel will be between the Mesh Portal and the controller, not the Mesh Point and the controller.

Services	Description	CSPs Accessed (see section 6 below for a complete description to each CSP and the associated cryptographic algorithms)
Creation/use of secure mesh channel ³	The module requires secure connections between mesh points using 802.11i	1, 25 (read) 26, 27, 28, 29, 30 (read/write)
Zeroization	The cryptographic keys stored in SDRAM memory can be zeroized by rebooting the module. The cryptographic keys (IKEv1 Pre-shared key and 802.11i Pre-Shared Key) stored in the flash can be zeroized by using command 'ap wipe out flash' or by overwriting with a new secret. The 'no' command in the CLI can be used to zeroize IKE, Ipsec CSPs. Please See CLI guide for details. The other keys/CSPs (RSA/ECDSA public key/private key and certificate) stored in Flash memory can be zeroized by using command 'ap wipe out flash'.	All CSPs (not including the Factory CA Public Key) will be destroyed.
Openflow Agent	Agent run on device for use with Mobility Master SDN. Leveraged by the SDN for discovering of hosts and networks, configuration of networks, and collection of statistics.	None

Table 13 - Crypto Officer Services

4.2.2 User Services

The User role for Remote AP FIPS mode and Control Plane Security (CPSec) Protected AP FIPS mode supports the same services listed in the Section 4.2.1 Crypto Officer Services.

The User role for Mesh Portal FIPS mode and Mesh Point FIPS mode supports the services listed in Section 4.2.3 Wireless Client Role.

³ This service is only applicable in the Mesh Portal FIPS mode and Mesh Point FIPS mode. It is not applicable in Control Plane Security (CPSec) Protected AP FIPS mode and Remote AP FIPS mode.

4.2.3 Wireless Client Services

The following services are provided for the Wireless Client role in Remote AP FIPS mode, CPSec protected AP FIPS mode, Mesh Portal FIPS mode and Mesh Point FIPS mode.

Service	Description	CSPs Accessed (see section 6 below for a complete description to each CSP and the associated cryptographic algorithms)
Generation and use of 802.11i cryptographic keys	In all modes, the links between the module and wireless client are secured with 802.11i.	1, 25 (read) 26,27,28,29,30 (read/write)
Use of 802.11i Pre-shared secret for establishment of IEEE 802.11i keys	When the module is in advanced Remote AP configuration, the links between the module and the wireless client are secured with 802.11i. This is authenticated with a shared secret only.	1, 25 (read)
Wireless bridging services	The module bridges traffic between the wireless client and the wired network.	None

Table 14 - User Services (Wireless Client Services)

4.2.4 Unauthenticated Services

The module provides the following unauthenticated services, which are available regardless of role.

- System status – module LEDs
- Reboot module by removing/replacing power
- Self-test and initialization at power-on.

4.2.5 Services Available in Non-FIPS Mode

- All of the services that are available in FIPS mode are also available in non-FIPS mode.
- If not operating in the Approved mode as per the procedures in section 8, then non-Approved algorithms and/or sizes are available..
- Upgrading the firmware via the console port.
- Debugging via the console port.

4.2.6 Non-Approved Services Disallowed in FIPS Mode

- The Suite-B (bSec) protocol is a pre-standard protocol that has been proposed to the IEEE 802.11 committee as an alternative to 802.11i.
- WPA3
- WPA-2 Multiple Pre-Shared Key (MPSK), where every client connected to the WLAN SSID may have its own unique PSK.
- IPSec/IKE using Triple-DES

5 Cryptographic Algorithms

The firmware in each module contains the following cryptographic algorithm implementations/crypto libraries to implement the different FIPS approved cryptographic algorithms that will be used for the corresponding security services supported by the module in FIPS mode: NOTE: The modes listed for each algorithm are only those actually used by the module (additional modes may have been tested during CAVS testing and not currently used).

- ArubaOS OpenSSL Module algorithm implementation
- ArubaOS Crypto Module algorithm implementation
- ArubaOS UBOOT Bootloader algorithm implementation
- Aruba AP Hardware algorithm implementation

Below are the detailed lists for the FIPS approved algorithms and the associated certificate implemented by each crypto library

ArubaOS OpenSSL					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
5266	AES	FIPS 197, SP 800-38A	ECB, CBC, CFB (128only), CTR (192, 256, ext only)	128, 192, 256	Data Encryption/Decryption
1739	CVL RSASP1 PKCS 1.5	FIPS 186-4		MOD 2048	RSA
1738	CVL IKEv1	SP 800-135 Rev1	IKEv1(DSA, PSK 2048, SHA-256, 384),	MOD 2048	Key Derivation
2017	DRBG	SP 800-90A	AES CTR	256	Deterministic Random Number Generation
1375	ECDSA	186-4	PKG, SigGen, SigVer	P256, P384	Digital Key Generation, Signature Generation and Verification
3485	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
181	KBKDF	SP 800-108	CTR	HMAC-SHA1, HMAC-SHA256, HMAC-SHA384	Deriving Keys
1366	DSA	FIPS 186-4		2048	Key Generation, PQG Generation
2816	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification

2816	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048	Key Gen, Digital Signature Generation and Verification
4236	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only		Message Digest
2664	Triple-DES ⁴	SP 800-67 Rev2	TEBC, TCBC	192	Data Encryption/Decryption
AES 5266 HMAC 3485	KTS	SP 800-38F	AES-CBC ⁵	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec

Table 15 – Algorithm Certificates (ArubaOS OpenSSL)

Note:

- RSA (non-compliant with the following functions:)
 - ❖ FIPS186-2:
 - ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537)
 - ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024, SHS: SHA-1/SHA-256/SHA-384/SHA-512, 2048, SHS: SHA-1
- ECDSA (non-compliant with the following functions:)
 - ❖ FIPS186-2:
 - SIG(gen): CURVES(P-256 P-384), SHS: SHA-1

ArubaOS Crypto Module					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
5265	AES	FIPS 197, SP 800-38A SP800-38D	CBC, GCM, CTR (ext only)	128, 192, 256	Data Encryption/Decryption
1736	CVL IKEv1, IKEv2	SP800-135 Rev1	IKEv1(DSA, PSK 2048, SHA-256, 384), IKEv2(2048 SHA-256, 384)		Key Derivation
1737	CVL RSASP1	186-4	2048 PKCS #1.5		Key Gen, SigVer, SigGen
1374	ECDSA	186-4	PKG, SigGen, SigVer (P-256, 384, SHA 1, 256, 384,	P256, P384	PKG, Digital Signature Generation and Verification

⁴ In FIPS Mode, Triple-DES is only used in the Self-Tests and with the KEK.

⁵ key establishment methodology provides between 128 and 256 bits of encryption strength

			512		
1365	DSA	186-4	PQG, KeyGen	2048	Digital Signature Generation and Verification
3484	HMAC	FIPS 198-1	HMAC-SHA1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512	112, 126, 160, 256	Message Authentication
2815	RSA	FIPS 186-2	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	1024 (legacy SigVer only), 2048	Digital Signature Verification
2815	RSA	FIPS 186-4	SHA-1, SHA-256, SHA-384, SHA-512 PKCS1 v1.5	2048, 1024 (legacy SigVer only)	Key Generation, Digital Signature Generation and Verification
4235	SHS	FIPS 180-4	SHA-1, SHA-256, SHA-384, SHA-512 Byte Only		Message Digest
2663	Triple-DES ⁶	SP 800-67 Rev2	TCBC	192	Data Encryption/Decryption
AES 5265	KTS	SP 800-38F	AES-GCM ⁷	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec
AES 5265 HMAC 3484	KTS	SP 800-38F	AES-CBC ⁸	128, 192, 256	Key Wrapping/Key Transport via IKE/IPSec

Table 16 – Algorithm Certificates (ArubaOS Crypto Module)

Note:

- The algorithms in the table are not used when the module is configured into the Mesh Point FIPS mode
- RSA (non-compliant with the following functions:)
 - ❖ FIPS186-2:
 - ALG[ANSIX9.31]: Key(gen)(MOD: 1024 PubKey Values: 65537)
 - ALG[RSASSA-PKCS1_V1_5]: SIG(gen): 1024, SHS: SHA-1/SHA-256/SHA-384/SHA-512, 2048, SHS: SHA-1
- ECDSA (non-compliant with the following functions:)
 - ❖ FIPS186-2:
 - SIG(gen): CURVES(P-256 P-384), SHS: SHA-1

⁶ In FIPS Mode, Triple-DES is only used in the Self-Tests

⁷ key establishment methodology provides between 128 and 256 bits of encryption strength

⁸ key establishment methodology provides between 128 and 256 bits of encryption strength

ArubaOS UBOOT Bootloader					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
2395 & 3111	RSA	FIPS 186-4	SHA-1, SHA256	2048	Digital Signature Verification
3633 & 4685	SHS	FIPS 180-4	SHA-1, SHA-256 Byte Only		Message Digest

Table 17 – Algorithm Certificates (Bootloader)

NOTE: Only Firmware signed with SHA-256 is permitted in the Approved mode. Digital signature verification with SHA-1, while available within the module, shall only be used while in the non-Approved mode.

Aruba AP Hardware					
CAVP Certificate #	Algorithm	Standard	Mode/Method	Key Lengths, Curves, Moduli	Use
5412 and 5664	AES	FIPS 197, SP 800-38A SP800-38C	ECB, CCM, GCM(used for self-test only)	128, 256	Data Encryption/Decryption

Table 18 – Algorithm Certificates (AP Hardware)

Non-FIPS Approved Algorithms Allowed in FIPS Mode

- NDRNG (used solely to seed the Approved DRBG)
- Diffie-Hellman (key agreement; key establishment methodology provides 112 bits of encryption strength)
- EC Diffie-Hellman (key agreement; key establishment methodology provides 128 or 192 bits of encryption strength)

NOTE: IKEv1 and IKEv2 protocols have not been reviewed or tested by the CAVP and CMVP.

Non-FIPS Approved Cryptographic Algorithms used only in Non-FIPS 140 Mode

The cryptographic module implements the following non-approved algorithms that are not permitted for use, and are not used, in the FIPS 140-2 mode of operations:

- DES
- HMAC-MD5
- MD5
- RC4
- RSA (non-compliant less than 112 bits of encryption strength)
- Null Encryption (Disallowed by Policy)
- Triple-DES as used in IKE/IPSec (Disallowed by Policy)

Note: DES, MD5, HMAC-MD5 and RC4 are used for older versions of WEP in the non-approved mode

6 Critical Security Parameters

The following Critical Security Parameters (CSPs) are used by the module (unless explicitly specified, a CSP is applicable to all approved modes of operation):

#	Name	Algorithm/Key Size	Generation/Use	Storage	Zeroization
General Keys/CSPs					
1	Key Encryption Key (KEK) – Not considered a CSP	Triple-DES (192 bits)	Hardcoded during manufacturing. Used only to obfuscate keys stored in the flash, not for key transport. (3 Key, CBC)	Stored in Flash memory (plaintext)	The zeroization requirements do not apply to this key as it is not considered a CSP.
2	DRBG entropy input	SP 800-90a CTR_DRBG (512 bits)	Entropy inputs to DRBG function used to construct the DRBG seed. 64 bytes are gotten from the entropy source on each call by any service that requires a random number.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
3	DRBG seed	SP 800-90a CTR_DRBG (384-bits)	Input to the DRBG that determines the internal state of the DRBG. Generated using DRBG derivation function that includes the entropy input from the entropy source.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
4	DRBG Key	SP 800-90a CTR_DRBG (256 bits)	This is the DRBG key used for SP 800-90a CTR_DRBG.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
5	DRBG V	SP 800-90a CTR_DRBG V (128 bits)	Internal V value used as part of SP 800-90a CTR_DRBG.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
6	Diffie-Hellman private key	Diffie-Hellman Group 14 (224 bits)	Generated internally by calling FIPS approved DRBG (Cert. #2017) to derive Diffie-Hellman shared secret used in both IKEv1 and IKEv2.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

#	Name	Algorithm/Key Size	Generation/Use	Storage	Zeroization
7	Diffie-Hellman public key	Diffie-Hellman Group 14 (2048 bits)	Derived internally in compliance with Diffie-Hellman key agreement scheme. Used for establishing DH shared secret.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
8	Diffie-Hellman shared secret	Diffie-Hellman Group 14 (2048 bits)	Established during Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
9	EC Diffie-Hellman private key	EC Diffie-Hellman (Curves: P-256 or P-384).	Generated internally by calling FIPS approved DRBG (Cert #2017) during EC Diffie-Hellman Exchange. Used for establishing ECDH shared secret.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
10	EC Diffie-Hellman public key	EC Diffie-Hellman (Curves: P-256 or P-384).	Derived internally in compliance with EC Diffie-Hellman key agreement scheme. Used for establishing ECDH shared secret.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
11	EC Diffie-Hellman shared secret	EC Diffie-Hellman (Curves: P-256 or P-384)	Established during EC Diffie-Hellman Exchange. Used for deriving IPSec/IKE cryptographic keys.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
12	Factory CA Public Key	RSA (2048 bits)	This is RSA public key. Loaded into the module during manufacturing. Used for Firmware verification.	Stored in TPM	Since this is a public key, the zeroization requirements do not apply
IPSec/IKE⁹					

⁹ Not used in Mesh Point modes of operation

#	Name	Algorithm/Key Size	Generation/Use	Storage	Zeroization
13	IKEv1 Pre-shared secret ¹⁰	Shared secret (8 - 64 ASCII or 64 HEX characters)	Entered by CO role. Used for IKEv1 peers authentication.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash' or by overwriting with a new secret
14	skeyid	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv1 peers. It was established via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving other keys in IKEv1 protocol implementation.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module.
15	skeyid_d	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv1 peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv1). Used for deriving IKEv1 session authentication key.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
16	SKEYSEED	Shared Secret (160/256/384 bits)	A shared secret known only to IKEv2 peers. It was derived via key derivation function defined in SP800-135 KDF (IKEv2) and it will be used for deriving other keys in IKEv2 protocol.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting module by the
17	IKE session authentication key	HMAC-SHA-1/256/384 (160/256/384 bits)	The IKE session (IKE Phase I) authentication key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IKEv1/IKEv2 payload integrity verification.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

¹⁰ Applicable only to Remote AP and Mesh Portal modes

#	Name	Algorithm/Key Size	Generation/Use	Storage	Zeroization
18	IKE session encryption key	AES (128/192/256 bits, CBC)	The IKE session (IKE Phase I) encrypt key. This key is derived via key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IKE payload protection.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
19	IPSec session encryption keys	AES (CBC) and AES-GCM (128/192/256 bits)	The IPsec (IKE phase II) encryption key. This key is derived via a key derivation function defined in SP800-135 KDF (IKEv1/IKEv2). Used for IPsec traffics protection. IPsec session encryption keys can also be used for the Double Encrypt feature.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
20	IPSec session authentication keys	HMAC-SHA-1 (160 bits)	The IPsec (IKE Phase II) authentication key. This key is derived via using the KDF defined in SP800-135 KDF (IKEv1/IKEv2). Used for IPsec traffics integrity verification.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
21	IKE RSA Private Key	RSA private key (2048 bits)	This is the RSA private key. This key is generated by the module in compliance with FIPS 186-4 RSA key pair generation method. In both IKEv1 and IKEv2, DRBG (Cert. #2017) is called for key generation. It is used for RSA signature signing in either IKEv1 or IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash'
22	IKE RSA public key	RSA public key (2048 bits)	This is the RSA public key. This key is derived in compliance with FIPS 186-4 RSA key pair generation method in the module. It is used for	Stored in Flash memory (plaintext)	Zeroized by using command 'ap wipe out flash'

#	Name	Algorithm/Key Size	Generation/Use	Storage	Zeroization
			RSA signature verification in either IKEv1 or IKEv2. This key can also be entered by the CO.		
23	IKE ECDSA Private Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA private key. This key is generated by the module in compliance with FIPS 186-4 ECDSA key pair generation method. In IKEv2, DRBG (Cert #2017) is called for key generation. It is used for ECDSA signature signing in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash'.
24	IKE ECDSA Public Key	ECDSA suite B (Curves: P-256 or P-384)	This is the ECDSA public key. This key is derived in compliance with FIPS 186-4 ECDSA key pair generation method in the module. It is used for ECDSA signature verification in IKEv2. This key can also be entered by the CO.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash'
802.11i¹¹					
25	802.11i Pre-shared secret	Shared secret (8-63 ASCII characters, or 64 HEX characters)	Entered by CO role. Used for 802.11i client/server authentication.	Stored in Flash memory obfuscated with KEK	Zeroized by using command 'ap wipe out flash' or by overwriting with a new secret.
26	802.11i Pair-Wise Master key (PMK)	Shared secret (256 bits)	The PMK is transported to the module, protected by IPSec secure tunnel. Used to derive the Pairwise Transient Key	Stored in SDRAM (plaintext)	Zeroized by rebooting the module

¹¹ While operating in Mesh Point or Mesh Portal mode, the AP will only use PSK for 802.11. RAP and CPsec modes use both Certificate-based and PSK-based 802.11

#	Name	Algorithm/Key Size	Generation/Use	Storage	Zeroization
			(PTK) for 802.11i communications.		
27	802.11i Pairwise Transient Key (PTK)	HMAC (384 bits)	This key is used to derive 802.11i session key by using the KDF defined in SP800-108.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
28	802.11i session key	AES-CCM (128 bits)	Derived during 802.11i 4-way handshake by using the KDF defined in SP800-108 then used as the session key.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
29	802.11i Group Master Key (GMK)	Shared secret (256 bits)	Generated by calling DRBG (Cert. #2017). Used to derive 802.11i Group Transient Key GTK.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module
30	802.11i Group Transient Key (GTK)	AES-CCM (256 bits)	Derived from 802.11i GMK by using the KDF defined in SP800-108. The GTK is the 802.11i session key used for broadcast communications protection.	Stored in SDRAM memory (plaintext)	Zeroized by rebooting the module

Table 19 - Critical Security Parameters

Please note that:

- AES GCM IV generation is performed in compliance with the Implementation Guidance A.5 scenario 1. FIPS approved DRBG (Cert. #2017) is used for IV generation and 96 bits of IV is supported).
- For keys identified as being "Generated internally by calling FIPS approved DRBG", the generated seed used in the asymmetric key generation is an unmodified output from the DRBG.
- The module generates a minimum of 256 bits of entropy for use in key generation.
- In Remote AP FIPS mode, all CSPs are applicable.
- In CPSec Protected AP FIPS mode, the IKEv1 PSK CSPs are not applicable.
- In Mesh Point FIPS modes, all IPSec/IKE CSPs are not applicable.
- CSPs labeled as "Entered by CO" are transferred into the module from the Mobility Controller via IPSec.

7 Self-Tests

The module performs Power On Self-Tests regardless the modes (non-FIPS mode, Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode, Mesh Portal FIPS mode or Mesh Point FIPS mode). In addition, the module also performs Conditional tests after being configured into either Remote AP FIPS mode, Control Plane Security (CPSec) Protected AP FIPS mode Mesh Portal FIPS mode or Mesh Point FIPS mode. In the event any self-test fails, the module enters an error state, logs the error, and reboots automatically.

The module performs the following **Power On Self-Tests**:

ArubaOS OpenSSL Module:

- SHA (SHA-1, SHA-256, SHA-384, SHA-512) KATs
- HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) KATs
- Triple-DES (encrypt/decrypt) KATs
- AES (Encrypt/Decrypt) KATs
- ECDSA (Sign/Verify) KATs
- RSA (Sign/Verify) KATs
- DSA (Sign/Verify) KATs
- DRBG KATs
- ECDH (P-256) KAT
- DH (2048) KAT
- KDF108 KAT

ArubaOS Crypto Module:

- SHA (SHA-1, SHA-256, SHA-384, SHA-512) KATs
- HMAC (HMAC-SHA-1, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512) KATs
- AES (Encrypt/Decrypt) KATs
- AES-GCM (Encrypt/Decrypt) KATs
- Triple-DES (Encrypt/Decrypt KATs)
- ECDSA (Sign/Verify) KATs
- RSA (Sign/Verify) KATs
- DSA (Sign/Verify) KATs
- ECDH (P-256, P-384) Pairwise Consistency Tests
- DH (2048) Pairwise Consistency Tests

ArubaOS UBOOT Bootloader Module:

- Firmware Integrity Test: RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256 (the integrity test is the KAT)

Aruba AP Hardware algorithm implementation power on self-tests:

- AES-CCM (encrypt/decrypt) KATs
- AES-GCM (encrypt/decrypt) KATs
- AES-ECB (encrypt/decrypt) KATs

The following **Conditional Tests** are performed in the module:

ArubaOS OpenSSL Module algorithm implementation:

- CRNG Test to Approved RNG (DRBG)
- CRNG test to NDRNG
- SP800-90A Section 11.3 Health Tests for CTR_DRBG (Instantiate, Generate and Reseed).
- ECDSA Pairwise Consistency Test
- RSA Pairwise Consistency Test

ArubaOS Crypto Module algorithm implementation:

- RSA Pairwise Consistency Test
- ECDSA Pairwise Consistency Test

ArubaOS UBOOT Bootloader Module algorithm implementation:

- Firmware Load Test - RSA PKCS#1 v1.5 (2048 bits) signature verification with SHA-256

These self-tests are run for the hardware cryptographic implementation as well as for the Aruba OpenSSL and ArubaOS cryptographic module implementations.

Self-test results are written to the serial console.

In the event of a KATs failure, the AP logs different messages, depending on the error.

For an ArubaOS OpenSSL AP module and ArubaOS cryptographic module KAT failure:

AP rebooted [DATE][TIME] : Restarting System, SW FIPS KAT failed

For an AES Atheros hardware POST failure:

Starting HW SHA1 KAT ...Completed HW SHA1 AT

Starting HW HMAC-SHA1 KAT ...Completed HW HMAC-SHA1 KAT

Starting HW AES KAT ...Restarting system.

8 Secure Operation

The module can be configured to be in the following FIPS approved modes of operations via corresponding Aruba Mobility Controllers that have been certified to FIPS level 2:

- Remote AP FIPS mode – When the module is configured as a Remote AP, it is intended to be deployed in a remote location (relative to the Mobility Controller). The module provides cryptographic processing in the form of IPSec for all traffic to and from the Mobility Controller.
- Control Plane Security (CPSec) Protected AP FIPS mode – When the module is configured as a Control Plane Security protected AP it is intended to be deployed in a local/private location (LAN, WAN, MPLS) relative to the Mobility Controller. The module provides cryptographic processing in the form of IPSec for all Control traffic to and from the Mobility Controller.
- Mesh Portal FIPS mode – When the module is configured in Mesh Portal mode, it is intended to be connected over a physical wire to the mobility controller. These modules serve as the connection point between the Mesh Point and the Mobility Controller. Mesh Portals communicate with the Mobility Controller through IPSec and with Mesh Points via 802.11i session. The Crypto Officer role is the Mobility Controller that authenticates via IKEv1/IKEv2 pre-shared key or RSA/ECDSA certificate authentication method, and Users are the "n" Mesh Points that authenticate via 802.11i preshared key.
- Mesh Point FIPS mode – an AP that establishes all wireless path to the Mesh portal in FIPS mode over 802.11 and an IPSec tunnel via the Mesh Portal to the controller.

In addition, the module also supports a non-FIPS mode – an un-provisioned AP, which by default does not serve any wireless clients. The Crypto Officer must first enable and then provision the AP into a FIPS AP mode of operation. Only firmware updates signed with SHA-256/RSA 2048 are permitted. The user is responsible for zeroizing all CSPs when switching modes.

The instructions for provisioning the APs are in the User Guide which is provided in Section 8.5 below. An important point in the Aruba APs is that to change configurations from any one mode to any other mode requires the module to be re-provisioned and rebooted before any new configured mode can be enabled.

The access point is managed by an Aruba Mobility Controller in FIPS mode, and access to the Mobility Controller's administrative interface via a non-networked general purpose computer is required to assist in placing the module in FIPS mode. The controller used to provision the AP is referred to as the "staging controller". The staging controller must be provisioned with the appropriate firmware image for the module, which has been validated to FIPS 140-2, prior to initiating AP provisioning.

Once the AP has been provisioned, it is considered to be in FIPS mode provided that the guidelines on services, algorithms, physical security and key management found in this Security Policy are followed.

8.1 Verify that the module is in FIPS mode

When connecting the AP to the controller for initial configuration, the Mobility Controller will provide the AP with a FIPS firmware image for use. While running this image, the AP will be compliant with FIPS requirements provided that the guidelines on services, algorithms, physical security and key management found in this Security Policy are followed. To verify that the image is being run, the CO can enter 'show ap image' on the controller to verify the correct image is present on the device. Additionally, the CO can enter 'fips enable' if connecting to a non-FIPS enabled Controller to ensure the Access Point only accepts FIPS approved cryptography.

8.2 Full Documentation

Can be found at:

<https://support.arubanetworks.com/Documentation/tabid/77/DMXModule/512/Default.aspx?EntryId=34189>

8.3 Disallowed FIPS Mode Configurations

When you enable FIPS mode, the following configuration options are forcibly disallowed:

- All WEP features
- WPA
- TKIP mixed mode
- Any combination of DES, MD5, and PPTP

When you enable FIPS mode, the following configuration options are disallowed by policy:

- USB CSR-Key Storage
- Telnet
- Firmware images signed with SHA- 1
- Enhanced PAPI Security
- Null Encryption
- EAP-TLS Termination
- IPSec/IKE using Triple-DES